1:17 MJ 9011

AFFIDAVIT OF MICHAEL P. BRIAN

I, Michael P. Brian, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent (SA) with the Federal Bureau of Investigation ("FBI") for approximately eighteen years. During this time, I have been assigned to numerous investigations involving complex computer crimes. I am currently assigned to the FBI Cleveland Division Cyber Crimes Squad and am responsible for investigations involving computer-related offenses. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information. In addition to my work experience, I have received specialized training in the field of computer crime investigation from the FBI and others.

2. I submit this affidavit in support of a criminal complaint charging PHILLIP ROMAN DURACHINSKY, date of birth [redacted], with a violation of Title 18, USC, Section 1030(a)(5)(A) and 1030(c)(4)(A)(i)(VI), that is, knowingly causing the transmission of a program, information, code, and command, and as a result of such conduct, intentionally causing damage without authorization, to ten or more protected computers.

3. The statements contained in this affidavit are based upon my own investigation, information provided by other Special Agents and personnel of the FBI involved in this investigation, and my personal experience with computer related offenses. Since this affidavit is being submitted for the limited purpose of securing the requested complaint, I have not included each and every fact known to me concerning this investigation.

PROBABLE CAUSE

4. On January 4, 2017, Case Western Reserve University (CWRU) was contacted by a third party regarding network scanning and an infected system on the third party's network. The third party provided CWRU indicators of compromise, i.e., computer forensic artifacts indicating a computer infection, which were used in the malware communications found on the third party system. The third party stated that it believed that because of the communication between the third party's infected computer and the CWRU system, the CWRU system was also likely compromised.

5. On January 5, 2017, CWRU contacted the Cleveland Division of the FBI related to the notification from the third party and confirmed that an intrusion had occurred on the CWRU network. CWRU identified over 100 computers at CWRU with active Internet connections as being infected with the malware. DURACHINSKY did not have authorization from CWRU, or from the owners of the infected CWRU computers, to damage those protected computers by accessing them and installing malware.

6. On January 6, 2017, the FBI interviewed CWRU Information Technology (IT) security personnel and imaged an infected computer. The FBI's review of the image confirmed that computers at CWRU had been compromised for several years.

7. CWRU determined that an IP address associated with the malware that had infected the CWRU computers had also been used to access the alumni email account of CWRU alumnus PHILLIP ROMAN DURACHINSKY, date of birth [redacted].

8. On January 18, 2017, a laptop was obtained by the FBI which belonged to PHILLIP ROMAN DURACHINSKY. DURACHINSKY's laptop contained the client control software for the above described malware.

9. Further investigation revealed that DURACHINSKY also infected a number of other universities and institutions with the same or similar malware that infected CWRU. DURACHINSKY also did not have authorization to damage the computers of other infected universities and their computer users by installing malware.

10. Further, DURACHINSKY's laptop contained files, logs, notes and other evidence of the installation of malware on more than 10 computers for the period of January 18, 2016, through January 18, 2017. The malware allowed DURACHINSKY to access data stored on the infected computers including Personal Identifying Information (PII) such as social security numbers and addresses, documents belonging to the computer owners, usernames, and passwords. It further allowed DURACHINSKY to collect data in real time from the infected machine and from computers and digital media connected to it. DURACHINSKY lacked the authorization from either CWRU or the infected CWRU computer users to access their computers, or to damage their computers by installing the malware.

CONCLUSION

11. Based on the foregoing, there is probable cause to believe that on January 6, 2017, the defendant, PHILLIP ROMAN DURACHINSKY did knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization, to 10 or more protected computers during a 1-year period, in

1:17 MJ 9011

violation of 18 U.S.C. Section 1030(a)(5)(A) and 1030(c)(4)(A)(i)(VI).

Respectfully submitted,

Michael P. Brian
Special Agent
FBI

Subscribed and sworn to before me on 1.24.17, 2017.

WILLIAM H. BAUGHMAN, JR.
UNITED STATES MAGISTRATE JUDGE